International Journal of Science Engineering and Advance Technology, IJSEAT , Vol.3, Issue 10
ISSN 2321-6905
October 2015

International Journal of Science Engineering and Advance Technology

A New Technique For Authenticating Short Encrypted Messages

[1]M.Vamsi Krishna, [2]V.G.L.Narasamba, [3]N.Veeramani
[1]HOD & Professor, [2.]Professor &Guide, [3.]Final Year MTech Student
[1.2 3]Department of Computer Science and Engineering, Chaitanya Institute of Science and Technology, Madhavapatnam, Kakinada, East Godavari District, Andhara Pradesh, India.

ABSTRACT:

The best MACs in the cryptographic narrative are based on universal hashing. The major cause following the presentation benefit of worldwide hashing-based MACs is the fact that dispensation messages block by block by universal hash functions is orders of scale faster than dispensation them block by block using block ciphers or cryptographic hash functions. One of the major dissimilarity among unconditionally secure MACs based on universal hashing and computationally secure MACs based on universal hashing is the obligation to course the solid image with a cryptographic prehistoric in the latter class of MACs. The heavy cause behind our search is that by a common purpose MAC algorithm to validate replace messages in such systems might not be the as a rule resourceful solution and can direct to misuse of resources by now existing, that is, the refuge that is supply by the encryption algorithm.

KEYWORDS: Authentication, unconditional security, computational security, universal hash-function families, pervasive computing.

I. INTRODUCTION:

The make use ofof universal hash-function relations in the Carter- Wegman style is not controlled tointendof totally secure verification. Computationally protected MACs based on universal hash functions can be createwith two rounds of totalling. In the firstround, the memo to be authentic is packed inbya universal hash function. Then, in the second round, thepacked in image is procedure with a cryptographicfunction naturally a pseudorandom function1. Admired computationally protected universal hashing-based MACsembrace, but are not limited.To be sure, universal hashing-based MACs give superiorrecital when contrast to block cipher or cryptographichashing-based MACs. Given that universal hashfunctions are not cryptographic functions, the inspectionof several message-image pairs can disclose the value of thehashing key. Given that the hashing key is used continually incomputationally secure MACs, the introduction of the hashingkey will show the way to contravention the safety of the MAC.

II. RELATED WORK:

Anacceptedgroup of totallyprotectedverification is based on universal hash-function families, pioneered by Carter and Wegman. Becausethe revise of unconditionally secure message authentication based on universal hash functions has been draw research attention, both from the intend and investigation standpoints. In computationally secure MACs, keys can be used to confirm an arbitrary number of messages. That is, after harmonizing on a key, genuine users can swap overan subjective number of authenticated messages with the same key. Depending on the main building block used to put up them, computationally secure MACs can be classified into three main categories: block cipher based, cryptographic hash function based, or universal hash function family based.

III. LITERATURE REVIEW:

THE AUTHOR, Morris Dworkin**(ET .AL), AIM IN [1],** thiscounselspell out a message authentication code (MAC) algorithm based on a symmetric key block cipher. This block cipher-based MAC algorithm, called CMAC, may be used to make availableguarantee of the realism and, hence, the veracity of binary data.

THE AUTHOR, Krishna Kumar Venkatasubramanian **(ET .AL) AIM IN [2],** protect a person's time alone in ancompetent manner is very vital for decisive, life-saving

infrastructures like Body Sensor Networks (BSN). This paper presents a novel key agreement scheme which agrees to two sensors in a BSN to concur to a common key produce using electrocardiogram (EKG) signals. This EKG-based Key Agreement (EKA) schemeaspire to carry the "plug-n-play" concept to BSN safety whereby justorganize sensors on the subject can allowsafe communication, without need any form of initialization such as pre-deployment. Examination of the system based on real EKG data (obtained from MIT PhysioBank database) shows that keys resultant from EKA are: random, time variant, can be generated based on short-duration EKG measurements, the same for a given subject and dissimilar for separate individuals.

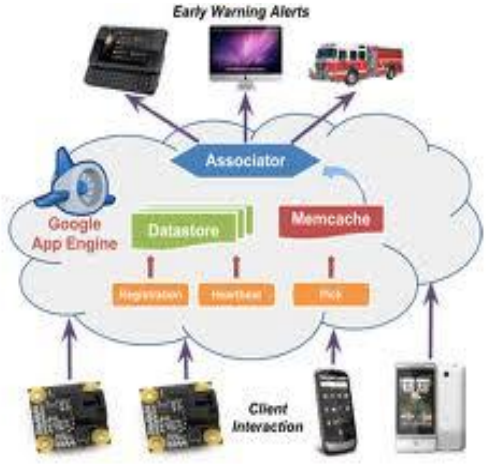
IV. PROBLEM DEFINITION:

Completelysheltered universal hashing-based MACs are cautiousawkward in mainly modern applications, due to the difficulty of managing one-time keys. Aconventional class of firmlysafeverification is based on worldwide hash-function families;lead the way by Carter and Wegman. Since then, the learn of entirelysafe message confirmation based on universal hash functions has been illustration research attention, both beginning the design and analysis standpoints.

V. PROPOSED APPROACH:

Thedetailis that the message to be authentic is also encrypted, with somesecure encryption algorithm, to put in on a short random string to be used in the confirmationprocedure. As the possibility strings used for unlike operations are self-governing, the authentication algorithm can gain from the effortlessness of without qualificationssafe authentication to let for sooner and additionalcapable authentication, with no the difficulty to handle one-time keys. In the immediatesystem, we make the addedstatement that the used encryption algorithm is block cipher based to furtherget better the computational cleverness of the first technique. The serioussourceat the back our question is that by means of a general purpose MAC algorithm to confirm exchanged messages in such systems strength not be the usuallycapable solution and can guide to waste of resources beforehand available, namely, the defence that is supply by the encryption algorithm.

VI. SYSTEM ARCHITECTURE:



VII. PROPOSED METHODOLOGY:

ADMIN:
The Admin needs to login by utilizing substantial client name and secret key. After login fruitful he have the capacity to do a few operations like rundown all client messages, list clients, list all aggressors, view versatile clients and logout.

LIST ALL USER MESSAGES:
The administration can examination rundown of all the client messages. In the event that the administrator click on the rundown all client messages catch then the server will put on demonstrate all rundown of all messages with their labels message ID, message to, message from, Mobile no, E-mail, title Name, Key utilized, MAC key, Date & time.

LIST USERS:
The Admin can examination rundown of all clients. Here all list clients are put away with the data, for example, client Image, User name, DOB, E -Mail, Mobile, Location and Secret Key.

LIST ALL ATTACKERS:
The administrator can vision all attackers list. The attackers points of interest are stores with the subtle elements, for example, Message ID, title name, key utilized, MAC key, Date & time, message. The administrator can likewise standpoint the portable clients with their labels client name, secret key, Email.

USER:
There are n quantities of clients present. Client ought to enroll to a demanding gathering past to doing any operations. After enlistment effective he needs to login by utilizing authority client name and watchword. After signed in he will do some procedure, for example, see my points of interest,

send message, perspective messages, demand for client access key, demand for message SK and MAC key, assault client messages and logout. In the event that client taps on my points of interest catch, then the server will offer answer to the client with their labels, for example, client Image, User name, DOB, E-mail, Mobile and Location.

SEND MESSAGE:
The client can send messages to one more client. To do this, client needs to enter the entrance key given by the administrator and give in, then client needs to enter the beneficiary name, title name and message, the message will be encoded and a MAC worth is created in light of the message content. This information will be put away in the information base.
VIEW MESSAGES:

The client can examination the all messages post then the server will offer answer to the client with their labels, for example, message ID, message to, message from, Mobile no, E-mail, title Name, Key utilized, MAC key, Date & time, message and legitimacy. To viewpoint the message content first client needs to get the message mystery key and message MAC key then client can download message.

CHECK MESSAGE VALIDITY:
The client can verify the message quality. To check the message quality the client needs to tap on the catch check message legitimacy and needs to enter the Message ID, title name and message MAC key. At that point message will demonstrate whether it is suitable on not.

ANDROID TEST BOOK:
The client can put in this application in his android versatile, after establishment to utilize this application client ought to enroll with the legitimate data. In the wake of flourishing enlistment client ought to login by the substantial client name and secret word. After signed in client can execute operations like perspective clients, perspective message pseudo irregular and MAC key, solicitation key. The administrator can too utilize this application in the android telephone; the administrator ought to login by the substantial client name and secret word. After signed in the administrator will accomplish the a few operations like view all clients, see all attackers, logout.

ALGORITHM

1)Message Encryption:

a) m be a short message that is to be transmitted to the planned collector in a classified way. For each message to be transmitted, an irregular nonce is choosed.

b) The concatenation of r and m goes to the encryption algorithm.

c) The nonce r is treated as the first plaintext block and is XORed with the initialization vector.

d) Construction of The first ciphertext block

$$c_1 = \mathcal{F}_{k\varepsilon}(IV \oplus r)$$

e) It is XORed with the second plaintext block, m in our construction, to produce the second ciphertext block.

$$c_2 = \mathcal{F}_{k\varepsilon}(c_1 \oplus m).$$

f) The key corresponding to the block cipher is then transmitted to the intended receiver as the ciphertext.

2) Message Authentication:

a) Authentication tag of message m

$$\tau \equiv m + r \pmod{2^N}.$$

b) Upon receiving the ciphertext, the intended receiver decrypts it to extract r and m.
c) The receiver can check the validity of the message

$$\tau \stackrel{?}{\equiv} m + r \pmod{2^N}.$$

d) If the integrity check of is satisfied, the message is considered authentic.
e) Otherwise the integrity of the message is denied

VIII. ENHANCEMENT:

Keeping in mind the end goal to enhance the execution of proposed system AES algorithm for encryption and decoding for message confirmation SHA is utilized proposed plans are indicated to be requests of greatness speedier, and expend requests

of extent less vitality than customary MAC algorithm.

IX. CONCLUSION:

Aninnovativemodus operandi for validate short encrypted messages is proposed. The statement that the messageto be above-board must also be encrypted is used to distribute a casual nonce to the intended receiver via the ciphertext. This allowed the devise of an authentication code those benefits from the plainness of categorically secure authentication without the need to administer one-time keys. The proposed schemes are exposed to be orders of magnitude faster, and devour orders of magnitude smaller amount energy than conventional MAC algorithms. So, they are additionalappropriate to be used in computationally unnatural mobile and enveloping devices.

X. FUTURE WORK:

Future exploration on enhance execution of proposed calculations as far as calculation and vitality utilization in computationally obliged portable and pervasive devices.

XI. REFERENCES:

[1] L. Carter and M. Wegman, "Universal Hash Functions,"J. Computer and System Sciences, vol. 18, no. 2, pp. 143-154, 1979.
[2] T. Helleseth and T. Johansson, "Universal Hash Functions fromExponential Sums over Finite Fields and Galois Rings," Proc. 16thAnn. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO '96),pp. 31-44, 1996.
[3] V. Shoup, "On Fast and Provably Secure Message AuthenticationBased on Universal Hashing," Proc. 16th Ann. Int'l Cryptology Conf.Advances in Cryptology (CRYPTO '96), pp. 313-328, 1996.
[4] B. Alomair, A. Clark, and R. Poovendran, "The Power of Primes:Security of Authentication Based on a Universal Hash-FunctionFamily," J. Math. Cryptology, vol. 4, no. 2, 2010.
[5] B. Alomair and R. Poovendran, "E-MACs: Towards More Secureand More Efficient Constructions of Secure Channels," IEEETrans. Computers, 2012.
[6] Federal Information Processing Standards (FIPS) Publication 113,Computer Data Authentication, FIPS, 1985.
[7] ISO/IEC 9797-1:1999 Standard, Information Technology – SecurityTechniques - Message Authentication Codes (MACs) - Part 1:Mechanisms Using a Block Cipher, ISO/IEC, 1999.
[8] M. Dworkin, "Recommendation for Block Cipher Modes ofOperation: The CMAC Mode for Authentication," 2005.
[9] T. Iwata and K. Kurosawa, "OMAC: One-Key CBC MAC," Proc.Int'l Conf. Fast Software Encryption (FSE '03), pp. 129-153, 2003.
[10] M. Bellare, R. Guerin, and P. Rogaway, "XOR MACs: NewMethods for Message Authentication Using Finite PseudorandomFunctions," Proc. 15th Ann. Int'l Cryptology Conf. Advances inCryptology (CRYPTO '95), pp. 15-28, 1995.
[11] P. Rogaway and J. Black, "PMAC," Proposal to NIST for aParallelizable Message Authentication Code, 2001.
[12] M. Bellare, J. Kilian, and P. Rogaway, "The Security of the CipherBlock Chaining Message Authentication Code," J. Computer andSystem Sciences, vol. 61, no. 3, pp. 362-399, 2000.
[13] B. Preneel and P. Van Oorschot, "On the Security of IteratedMessage Authentication Codes," IEEE Trans. Information Theory,vol. 45, no. 1, pp. 188-199, Jan. 1999.
[14] G. Tsudik, "Message Authentication with One-Way Hash Functions,"ACM SIGCOMM Computer Comm. Rev., vol. 22, no. 5,pp. 29-38, 1992.
[15] M. Bellare, R. Canetti, and H. Krawczyk, "Keying Hash Functionsfor Message Authentication," Proc. 16th Ann. Int'l Cryptology Conf.Advances in Cryptology (CRYPTO '96), pp. 1-15, 1996.

M VAMSI KRISHNA received the M Tech CS in Allahabad University, M.Tech (AI &R) degree in Andhra University, and Ph.D from Centurion University ,Odisha. Currently he is working as Professor & HOD in Department of Computer Science and Engineering. He has 15 years of experience in teaching. His research interests include Artificial intelligence, computer networks, image processing.

V.G.L.NARASAMBA received the MCA, M.Tech (CSE) degree from JNT University. Currently she is working as a professor in Department of Computer Science and Engineering. She has 9 years of experience in teaching. Her research interest include Computer Networks, operating system,

Advanced java, Web Technologies, Advanced Data Stractures, principles of programming languages.

N.Veeramani is a student of Chaitanya Institute of Science and Technology, Madhavapatnam, Kakinada, East Godavari District, Andhra Pradesh, India. Presently she is pursuing her M.Tech in Computer Science in this College and she received her BTECH from Ideal Institute of Technology in Kakinada, affiliated to JNT University, Kakinada in the year 2013.Her areas of interest in Computer Networks and Object Oriented Programming Languages and all current trends and techniques in Computer Science.